

Practical Quantum Coin Flipping

Anna Pappa,^{1,*} André Chailloux,² Eleni Diamanti,¹ and Iordanis Kerenidis²

¹*LTCI, CNRS - Télécom ParisTech, Paris, France*

²*LIAFA, CNRS - Université Paris 7, Paris, France*

(Dated: January 27, 2013)

We show that a single quantum coin flip with security guarantees that are strictly better than in any classical protocol is possible to implement with current technology. Our protocol takes into account all aspects of an experimental implementation like losses, multi-photon pulses emitted by practical photon sources, channel noise, detector dark counts and finite quantum efficiency. We calculate the abort probability when both players are honest, as well as the probability of one player forcing his desired outcome. For channel length up to 21 km, we achieve honest abort and cheating probability that are better than in any classical protocol. Our protocol is easy to implement using attenuated laser pulses, with no need for entangled photons or any other specific resources.

PACS numbers: 03.67.-a, 03.67.Dd

Introduction – Coin Flipping is a fundamental cryptographic primitive with numerous applications, where two distrustful parties separated by distance wish to agree on a random bit [1]. Classically, it is impossible to have a coin-flipping protocol with cheating probability less than 1, unless computational assumptions are considered. In other words, a dishonest player can force the outcome of the coin flip with probability 1. In the quantum model, where the two parties share a quantum channel, it was also proven that perfect coin flipping is information-theoretically impossible [2]. On the other hand, several quantum protocols have been proposed that achieve a cheating probability lower than 1 [3–5].

These results are important from a theoretical point of view, however they assume perfect implementation of the protocols. The situation is more subtle when we deal with realistic conditions encountered in experimental implementations, for example multi-photon pulses emitted by practical sources, losses and channel noise, since if taken into account they may render the protocols insecure in practice [3–7].

To study the security of practical coin flipping protocols, in addition to the cheating probability, we need to take into account the probability that the honest players abort the protocol. Hänggi and Wullschleger [8] gave tight bounds for the cheating probability p of any classical or quantum coin flipping protocol, where the honest players abort with probability H . Hence, the goal of any quantum implementation of coin flipping would be to achieve both honest abort and cheating probability strictly smaller than in any classical protocol.

Recently, protocols that address some of the issues that arise in experimental implementations have been proposed. A major step was taken by Berlin et al [9], who proposed a protocol that is completely impervious to losses and achieves cheating probability 0.9. In their theoretical analysis, they do not deal with noise and thus the honest abort probability is always zero. The main disadvantage of this protocol is that it becomes com-

pletely insecure in the presence of multi-photon pulses, i.e. when the implementation is based on an attenuated laser source rather than a perfect single-photon source. Subsequently, Berlin et al [10] implemented this protocol using a source of entangled qubits and hence avoiding multi-photon pulses. In order to deal with the noise present in the experiment, they defined a different primitive, *sequential coin flipping*, instead of a single coin flip, and conjectured that this primitive still remains impossible classically.

Chailloux [11] proposed an improved protocol with cheating probability 0.86. Last, Barrett and Massar [12] had introduced the primitive of string coin flipping, as an alternative to what they considered impossible to achieve experimentally, i.e. a single coin flip. However, this primitive turned out to be possible classically.

Our work – In the current letter, we present a quantum coin flipping protocol that can be implemented using today's technology and that has both honest abort and cheating probability provably lower than the ones achieved by any classical protocol [8]. Our protocol uses a standard attenuated laser source and we analyse how all practical aspects, like multi-photon pulses, channel noise, system loss, detector dark counts and finite quantum efficiency, affect the honest abort and cheating probability. We prove that for a single coin flip, if the noise is up to 2% and for channel length up to 21km, we can achieve at the same time honest abort probability ($\approx 1\%$) and cheating probability (≈ 0.91) strictly smaller than classically possible. We note that, similar to quantum key distribution protocols [13], our protocol is not completely impervious to losses, but can tolerate up to a certain amount of losses, which corresponds to distances in typical metropolitan area networks.

Protocol – Our protocol is a refinement of the one proposed by Berlin et al [9]; the main difference is that Alice sends K pulses instead of one, and uses an attenuated laser source to produce her states, instead of a perfect single-photon or an entangled-photon source:

1. Alice sends K photon pulses to Bob, where the number of photons in each pulse i follows the Poisson distribution with $p_i = e^{-\mu} \mu^i / i!$ and mean photon number μ . She prepares each pulse in the state $|\phi_{\alpha_i, c_i}\rangle$, $i = 1, \dots, K$, such that:

$$\begin{aligned} |\phi_{\alpha_i, 0}\rangle &= \sqrt{a}|0\rangle + (-1)^{\alpha_i} \sqrt{1-a}|1\rangle \\ |\phi_{\alpha_i, 1}\rangle &= \sqrt{1-a}|0\rangle - (-1)^{\alpha_i} \sqrt{a}|1\rangle \end{aligned}$$

where $\alpha_i \in_R \{0, 1\}$ is the basis and $c_i \in_R \{0, 1\}$ is the bit chosen by Alice.

2. Bob picks a measurement basis α'_i for every pulse. If his detectors do not click for any pulse, then he aborts. Else, let j the first pulse he detected.
3. Bob picks $c'_j \in_R \{0, 1\}$ and sends it to Alice, together with the index j .
4. Alice reveals α_j, c_j .
5. If $\alpha_j = \alpha'_j$, Bob checks that the outcome of his measurement is indeed $|\phi_{\alpha_j, c_j}\rangle$, otherwise he aborts.
6. If Bob has not aborted, then the outcome of the protocol is $b = c_j + c'_j$.

Honest Player Abort – Any amount of noise in an experimental implementation results in a non-zero honest abort probability. Here, we analyse how exactly noise and the other experimental parameters affect the honest abort probability in order to ensure that the protocol achieves a task which remains impossible classically. We note that a similar analysis can also be done for the Berlin et al. protocol. The situations where an honest abort might occur with some probability are the following:

1. Bob's detectors do not click in any of the K rounds of the coin flip. The abort probability is 1.
2. Bob's first detection is due to a dark count. The abort probability is $1/4$, since if $\alpha_j = \alpha'_j$ (step 5), he will abort with probability $1/2$ (dark count is totally random), else if $\alpha_j \neq \alpha'_j$ he will not abort.
3. The noise in the channel alters the state of the photon. The abort probability is $1/2$, since he will only abort if $\alpha_j = \alpha'_j$ (step 5).

The total honest abort probability is then:

$$\begin{aligned} H &= Z^K (1 - d_B)^K + \frac{1}{4} \sum_{i=1}^K (1 - d_B)^{i-1} d_B Z^i \\ &+ [1 - Z^K (1 - d_B)^K - \sum_{i=1}^K (1 - d_B)^{i-1} d_B Z^i] \frac{e}{2} \end{aligned}$$

where $Z = p_0 + (1 - p_0)(1 - F\eta)$: probability that no signal arrives at Bob's detectors; F : system transmission efficiency; η : detector finite quantum efficiency; d_B : probability of detector dark count; e : probability of wrong measurement outcome due to noise.

Malicious Alice – Alice's optimal cheating strategy in our protocol is the same as the one in the Berlin et al's protocol. We assume Alice to be all-powerful, which means that she controls all aspects of the implementation, including the errors in Bob's detectors. It is in her best interest to replace the lossy channel and Bob's faulty detectors with perfect ones, use a perfect single-photon source and send no vacuum states. Under these assumptions, honest Bob will always succeed in measuring the first pulse that Alice sends and disregard the following ones. Hence, Alice's optimal cheating strategy is to create some entangled state, send one qubit to Bob in the first pulse, wait for Bob to reply in step 3 and then perform some measurement in her part of the entangled state in order to decide what to reveal in step 4. This is no different from the cheating in Berlin et al's protocol, so the optimal cheating probability for Alice is $p_A = (3 + 2\sqrt{a(1-a)})/4$ [9].

Malicious Bob – We consider Bob to be all-powerful, meaning that he controls all aspects of the implementation, except for Alice's photon source. Again, it is in Bob's best interest to replace the lossy and noisy channel with a perfect one, in order to receive each time the correct state and maximize his cheating probability. Moreover, we assume he has perfect detectors and we also give him the ability to know the number of photons in each of the K pulses. Then, Bob's optimal strategy is to receive all K pulses and then perform some operation on the received qubits in order to maximize his information about Alice's bit c_j for some pulse j . It is important to note that honest Alice picks a new uniformly random bit c_j for each pulse j and hence Bob cannot combine different pulses in order to increase his information about a bit c_j .

To simplify our analysis, we assume that in the case where Bob has received at least two 2-photon pulses or a pulse with 3 or more photons, then he can cheat with probability 1. This probability is in fact very close to 1 and hence our upper bound on Bob's cheating probability is almost tight. We analyze the following events (in each event, the remaining pulses contain zero photons):

- A_1 : (all 0-photon pulses) The optimal cheating strategy for Bob is to try to guess Alice's bit, which happens with success probability $1/2$.
- A_2 : (at least one 1-photon pulse) The optimal cheating strategy for Bob is to measure in the computational basis (Helstrom measurement)[9, 14]. It is proven in [9] that this probability is equal to a .
- A_3 : (one 2-photon pulse) It can be proven that for our states the optimal measurement in a 2-photon pulse outputs the correct bit with probability equal to a .
- A_4 : (one 2-photon pulse, at least one 1-photon pulse) Bob will try to benefit from the 2-photon pulse (see discussion below), and if he fails, he will continue like in A_2 , since the pulses are independent.

Thus, we get an upper bound for the total probability of cheating Bob:

$$p_B \leq \sum_{i=1}^4 P(A_i) * P(\text{cheat}|A_i) + (1 - \sum_{i=1}^4 P(A_i)) * 1$$

Note that an honest Alice prepares the K pulses independently, which means that a measurement on any of them does not affect the rest. Consequently, Bob can measure each pulse independently, without affecting the remaining pulses. Moreover, the probability for each of these events depends on the protocol parameter K and on μ (which is controlled by Alice).

It remains to bound $P(\text{cheat}|A_4)$, i.e. the case where Bob has received one 2-photon pulse and some single photon pulses. Bob will try to profit from the two identical quantum states in one pulse. On one hand, he can perform the optimal distinguishing measurement on the two photons, which as we said earlier gives a correct answer with probability a . On the other hand, he can perform a conclusive measurement on the 2-photon pulse that with some probability will give a correct answer and with some probability will give no answer at all (in which case Bob can use one of the 1-photon pulses). In fact, none of these two strategies is optimal. In general, Bob will perform some measurement that with probability c will provide an answer, which will be correct with probability γ , and with probability $(1 - c)$ the measurement will provide no answer, in which case Bob will use a single-photon pulse to guess correctly with probability a . Hence,

$$P(\text{cheat}|A_4) = \max_M \{c\gamma + (1 - c)a\}$$

over all possible measurements of Bob.

Let M be the optimal measurement that provides with probability c an answer that is correct with probability γ and with probability $(1 - c)$ provides an answer that is correct with probability γ' . On one hand, we have that $\gamma' \geq 1/2$ (since Bob can always guess with probability $1/2$) and on the other hand this measurement cannot be correct with probability larger than a (since we know that the optimal measurement has probability a). Hence, we have $x \equiv c\gamma + (1 - c)1/2 \leq a$ from which we get that $c \geq 2x - 1$. Then, using the above equation we have:

$$\begin{aligned} P(\text{cheat}|A_4) = c\gamma + (1 - c)a &\leq x + (2 - 2x)(a - \frac{1}{2}) \\ &\leq -2a^2 + 4a - 1 \end{aligned} \quad (1)$$

Equation (1) provides an analytical upper bound on the cheating probability for event A_4 and hence we can now calculate the cheating probability p_B .

Fairness of the protocol – In order to have equal cheating probabilities, we adjust a so that $p_A = p_B$.

Experimental parameters – We have introduced a coin flipping protocol that takes into account all experimental parameters. In the following simulations, we use parameter values commonly referenced in the literature [15, 16], which can be implemented using today's technology.

The photon signals that Alice sends arrive with a probability F (transmission efficiency) at Bob's site, and they are detected with a probability η (detector quantum efficiency). For an optical channel, F is related to the channel absorption coefficient β , the channel length L and a distance-independent constant loss k , via the equation: $F = 10^{-(\beta L + k)/10}$. The values used in our simulations are shown in the following table.

Parameter		Value
Receiver constant loss [dB]	k	1
Absorption coefficient [dB/km]	β	0.2
Detection efficiency	η	0.2
Dark counts (per slot)	d_B	10^{-5}
Signal error rate	e	0.01

Note that we consider the probability of a signal and a dark count occurring simultaneously negligible.

Results – Our protocol requires a minimum honest abort probability equal to half of the probability of noise in the channel. We consider an acceptable honest abort probability smaller than 2%, thus by setting the honest abort probability to fixed values up to 0.02 for different channel lengths, we find the necessary rounds K and the optimal mean photon number μ that minimize the cheating probability for a fair protocol.

There is an inversely proportional relation between the honest abort probability and the optimal μ (Figure 1). The same holds for the number of rounds K in relation to the honest abort probability and for the same μ . When μ is increased in order to achieve the desired honest abort probability, the required number of rounds is reduced. In all our simulations, K did not exceed 15000.

In Figure 2 we plot our protocol's cheating probability versus the honest abort probability H for four different channel lengths, and compare this to the optimal classical cheating probability, which is equal to $1 - \sqrt{H/2}$ [8].

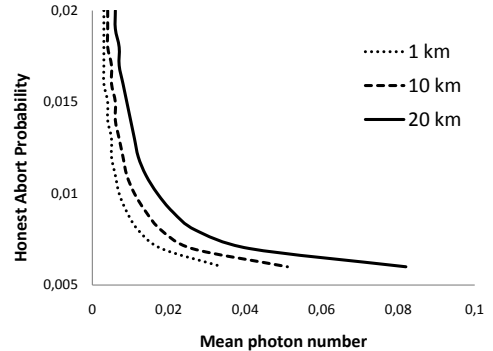


Figure 1: Quantum honest abort probability vs mean photon number μ for different channel lengths.

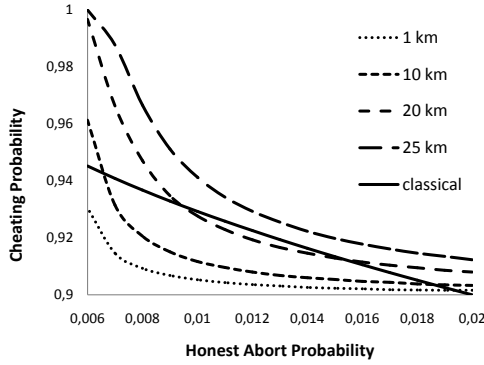


Figure 2: Quantum honest abort vs cheating probability for different channel lengths and comparison to the classical case.

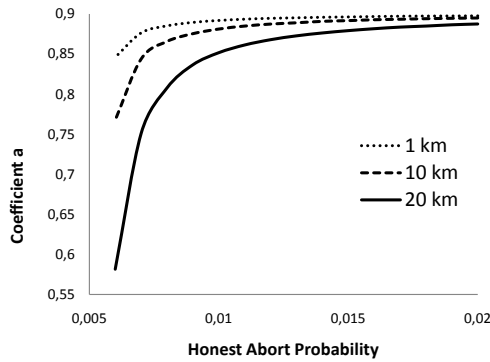


Figure 3: Quantum state coefficient vs honest abort probability.

For any length up to 21 km and honest abort probability smaller than 2%, we can find a μ such that the maximum cheating probability of our protocol is better than in the classical case. Figure 3 shows how the coefficient a of the protocol states changes in relation to the honest abort probability, for three different channel lengths.

Discussion – We have shown for the first time that flipping a single coin with security guarantees strictly stronger than in any classical protocol can be achieved with present quantum technology, and more precisely with a standard attenuated laser source. This implies that quantum information can be used beyond quantum key distribution (QKD), to achieve in practice more difficult cryptographic tasks in a model where the parties do not trust each other. We note that implementations of such tasks will be subject to the same issues related to the existence of side channels as in QKD (eg. [17]).

We observe that the maximal communication distance

that can be achieved is significantly smaller than in QKD [13]. In principle, we cannot expect to have the same results as in QKD, since the setting is much harder. Here, the adversary is the other player, so no cooperation is possible, thus excluding error-correction and privacy amplification. With the parameter values that we used, the limit to the channel length is 21 km. We can increase the channel length by improving the experimental parameters, in particular the signal error rate.

Even though Chailloux [11] proposed a protocol with lower cheating probability than the Berlin et al, it does not perform as well in the presence of noise.

Last, it is interesting to see if there is a way to reduce the effect of noise to the honest abort probability with current technology. We note that this seems hard, since any attempt of Alice to protect the qubits, via a repetition error correcting code for example, will immediately increase the cheating probability of Bob.

Acknowledgments – We acknowledge financial support from the ANR through projects CRYQ (ANR-09-JCJC-0067-01), FREQUENCY (ANR-09-BLAN-0410-01), and QRAC (ANR-08-EMER-012), and from the European Union through project QCS (grant 255961).

* Electronic address: anna.pappa@telecom-paristech.fr

- [1] M. Blum, in *CRYPTO* (1981), pp. 11–15.
- [2] H.-K. Lo and H. F. Chau, *Physica D* **120**, 177 (1998).
- [3] D. Aharonov, A. Ta-Shma, U. Vazirani, and A. Yao, in *Proceedings of STOC* (2000), pp. 705–714.
- [4] A. Ambainis, *Journal of Computer and System Sciences* **68**, 398 (2004).
- [5] A. Chailloux and I. Kerenidis, in *FOCS* (2009).
- [6] G. Molina-Terriza, A. Vaziri, R. Urzin, and A. Zeilinger, *Phys. Rev. Lett.* **94**, 040501 (2005).
- [7] A. T. Ngyuen, J. Frison, K. P. Huy, and S. Massar, *New Journal of Physics* **10**, 083087 (2008).
- [8] E. Hänggi and J. Wullschlegel, arXiv:1009.4741[quant-ph] (2010).
- [9] G. Berlin, G. Brassard, F. Bussi eres, and N. Godbout, *Phys. Rev. A* **80**, 062321 (2009).
- [10] G. Berlin, G. Brassard, F. Bussi eres, N. Godbout, J. Slater, and W. Tittel, arXiv:0904.3946v2[quant-ph] (2009).
- [11] A. Chailloux, in *AQIS* (2010).
- [12] J. Barrett and S. Massar, *Phys. Rev. A* **69**, 022322 (2004).
- [13] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Du ek, N. L utkenhaus, and M. Peev, *Rev. Mod. Phys.* **81**, 1301 (2009).
- [14] C. Helstrom, Academic Press, New York (1976).
- [15] G. Brassard, N. L utkenhaus, T. Mor, and B. Sanders, *Phys. Rev. Lett.* **85**, 1330 (2000).
- [16] N. L utkenhaus, *Phys. Rev. A* **61**, 052304 (2000).
- [17] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, *Nature Photonics* **4**, 686 (2010).